IN THE CLAIMS:

This listing of the claims replaces all prior versions and listings of the claims. Please amend claim 30 and add claims 39-47 as follows:

Claims 1-29. (canceled)

Claim 30. (currently amended) A security system comprising:

an activation token identifying system characteristics and specifying a threat level and at least one preset activation measure, wherein a system characteristic is one of the group of a hardware system, a service, a configuration of a service, a service execution platform, and a service version;

a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information; and

a second system configured to receive the activation token from a source external to the second system, the second system further configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the

second system, the activation measure configured to modify services executing at the second system.

Claim 31. (previously presented) The system of claim 30, further comprising a cryptographic means configured to verify at the second system that the first system is a trusted service.

Claim 32. (previously presented) The system of claim 30, further comprising a reporting means configured to report to a system administrator of the second system activation measures taken by the second system.

Claim 33. (previously presented) The system of claim 30, wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token.

Claim 34. (previously presented) The system of claim 30, further comprising a list of a plurality of trusted service providers from whom activation tokens are accepted by the second system.

Claim 35. (previously presented) The system of claim 30, wherein the at least one preset activation measure is shutting down a service affected by the specified threat level.

Claim 36. (previously presented) The system of claim 30, wherein the at least one preset activation measure is reconfiguring the functionality of a service affected by the specified threat level.

Claim 37. (previously presented) The system of claim 30, wherein the at least one preset activation measure is installing a patch for a service affected by the specified threat level.

Claim 38. (previously presented) The system of claim 30, wherein the at least one preset activation measure is alerting a system administrator.

Claim 39. (new) A security system comprising:

an activation token identifying system characteristics and specifying a threat level and at least one preset activation measure, wherein a system characteristic is one of the group of a hardware system, a service, a configuration of a service, a service execution platform, and a service version;

a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information, wherein the information publishers are external to the first system; and

a second system configured to determine whether the activation token is relevant by checking if actual

characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system, the activation measure configured to modify services executing at the second system.

Claim 40. (new) The system of claim 39, further comprising a cryptographic means configured to verify at the second system that the first system is a trusted service.

Claim 41. (new) The system of claim 39, further comprising a reporting means configured to report to a system administrator of the second system activation measures taken by the second system.

Claim 42. (new) The system of claim 39, wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token.

Claim 43. (new) The system of claim 39, further comprising a list of a plurality of trusted service providers from whom activation tokens are accepted by the second system.

Claim 44. (new) The system of claim 39, wherein the at least one preset activation measure is shutting down a service affected by the specified threat level.

Claim 45. (new) The system of claim 39, wherein the at least one preset activation measure is reconfiguring the functionality of a service affected by the specified threat level.

Claim 46. (new) The system of claim 39, wherein the at least one preset activation measure is installing a patch for a service affected by the specified threat level.

Claim 47. (new) The system of claim 39, wherein the at least one preset activation measure is alerting a system administrator.